

2025 Midwest Collegiate Cyber Defense Competition

Practical Hardening and Operational Security

Ethan Mitchell

### **PURPOSE OF THIS GUIDE**

This guide is intended for newcomers to the Collegiate Cyber Defense Competition (CCDC) who are serious about improving their technical depth. It assumes you are familiar with core networking and system administration concepts but need context for applying them under pressure. It is modeled after internal operations guides and security walkthroughs focusing more on **decision-making** and **reasoning** than spoon-fed instructions.

You won’t find every answer here—but you will find the **why**, the **what to look for**, and the **tools to investigate**. Use this to build your own workflow.

### **WHAT YOU'RE DEFENDING**

In CCDC, Windows Server machines are often scored on:

* **Active Directory / LDAP Auth** (usually authenticating Linux mail or user services)
* **DNS Resolution** (forwarding queries from outside the domain)

Your job isn’t just to “keep the lights green”—you need to:

* Harden your attack surface
* Maintain core functionality (scored services)
* Complete business-driven injects
* Detect, respond to, and report incidents

### 

### 

### **COMPETITION MINDSET**

Red Team has been doing this longer than you. They're looking for:

* Lazy configs
* Default credentials
* Known CVEs
* Services you forgot were running

What matters is how fast you detect, contain, and recover.

Start developing instincts like:

* “Why would this process run here?”
* “What just changed in the startup list?”
* “Why is LDAP talking to a random external IP?”

### **IMMEDIATE TRIAGE CHECKLIST (DO NOT SKIP)**

You only get one chance to catch default misconfigurations. Create a prioritized hit list:

1. **Lock Credentials**: Before enabling NIC, change known passwords.
2. **Verify Admin Access**: Ensure you have control of local/domain admin.
3. **Enumerate**: What roles/services are running? What’s exposed?
4. **Segment Access**: Who should be able to talk to what? Restrict as needed.
5. **Begin Logging**: If you can’t explain what happened later, you’re blind.

Use PowerShell to gain visibility:

Get-WindowsFeature | Where-Object Installed

Get-LocalUser | Format-Table

netstat -ano | findstr :3389

Don’t patch blindly. Don’t close ports you haven’t confirmed aren’t being scored. This isn’t a home lab. Every change affects points.

### **INCLUDED POWERSHELL SCRIPTS (EDIT BEFORE USE)**

These are example tools—not drop-ins. You should:

* Read them
* Understand what each does
* Modify them based on your threat model

#### Firewall Visibility & Lockdown – FW-Up-To-Date.ps1

Set-NetFirewallProfile -Profile Domain,Private,Public -Enabled True

Get-NetFirewallRule | Where-Object {$\_.Enabled -eq "False"} | Set-NetFirewallRule -Enabled True

➡️ Try rewriting this to only allow known IPs per service.

#### Process Snapshot – ProMon.ps1

Get-Process | Sort-Object CPU -Descending | Select-Object -First 15 | Format-Table Name,Id,CPU,StartTime

➡️ What else could you log here? Command line args? Parent PID?

#### Executable Audit – ExecMon.ps1

Get-ChildItem C:\Windows\Temp -Recurse -Include \*.exe | Select-Object Name,LastWriteTime,FullName

➡️ Modify to log this to file or run as a repeating task.

### **FIREWALL RULE STRATEGY (NOT JUST COPY/PASTE)**

Understand the expected flow of traffic:

* LDAP: Should only talk to the mail server
* DNS: Should only respond to scoring server queries

Example lockdown (edit these based on what’s hitting your box):

$MailIP = "192.168.1.10"

Set-NetFirewallRule -DisplayName "LDAP Inbound" -RemoteAddress $MailIP -Enabled True

➡️ Use Wireshark to capture incoming IPs before applying rules. Don't block scoring.

### **DETECTION MINDSET – USE THE RIGHT TOOLS**

You're not expected to be Splunk experts. But you are expected to:

* Check Event Viewer regularly
* Watch for new services/tasks/processes
* Monitor outbound traffic (proxy? tunneling?)

#### Tools to learn deeply:

* **Autoruns** – Startup entries
* **Process Explorer** – Parent/child process tracing
* **TCPView** – Real-time network session mapping
* **Wireshark** – DNS, LDAP, SMB, RDP traffic inspection

Don't just use them. Ask why a Red Teamer might abuse them.

### **DNS / AD SERVICE RECOVERY**

You’re expected to rebuild services under pressure. If DNS is wiped:

* Review Wireshark for scoring queries
* Recreate A records with expected IPs
* Use nslookup from scoring subnet (if allowed)

Don’t clone working records—understand what each does. Learn:

* Forward vs Reverse Lookup Zones
* What port 53 is used for
* What happens if recursion is disabled

### **FINAL NOTE**

If you’re reading this to “get the flag,” you’re missing the point.

This guide is meant to help you learn the *process* of system defense in a hostile, realistic environment. Ask questions, build tools, and challenge assumptions. You'll win more by learning than by surviving.

More advanced coverage (incident response, live IR scripting, policy injects, etc.) to follow.